SAVIYNT

Top Lessons in Higher Education Identity Security

A Primer on Solving Identity Governance Challenges for Today's Universities

Contents

Introduction

Universities and other higher education institutions are facing significant challenges. From vacated dorms and online classes to virtual graduation ceremonies, digitization programs are intersecting with pandemic countermeasures. Leaders must now balance a significantly changed operating environment with the need to protect their data while continuing to deliver world-class education and research programs.

Colleges and universities struggle with keeping students, faculty, and staff physically safe while navigating a path to protecting their data. With remote learning becoming an integral part of today's higher education experience, identity management is more crucial than ever.

The future of higher education will be increasingly digital. Digital transformation — from online learning and degree programs to growing interest in massive open online courses (MOOCS) — was already in full swing in institutions worldwide. This transformation, which has accelerated due to the pandemic, is challenging university administrators to prioritize students' digital experience while scaling to operate efficiently.

Universities must maintain a high level of data security and anticipate new risks, and identity governance is central to these efforts.

Yet many higher education IT and security teams are impeded by legacy Identity Governance and Administration (IGA) solutions that can create visibility challenges and require extensive coding and other manual steps before accounts can be provisioned or de-provisioned. The need to maintain a significant amount of on-premises infrastructure is also a challenge.

This report is a guide for IT and business leaders to overcome specific identity and access management challenges seen in the higher education sector.

The report also includes a real-world example of how one university implemented Saviynt's identity management platform to secure access and improve operations.

Identity Management in a Changing Digital Economy

In today's cloud and digital-first world, time-consuming, labor-intensive identity management processes are inefficient, burdensome, and create security risks of their own.

The digital economy is changing fast, and there is a need for identity management practices to keep pace. Managing identity in higher education (and most other sectors) also comes with unique challenges. Institutions have persona-based identity access requirements that evolve based on time, place, role, and the resource being accessed. IT and security teams must manage a multitude of joiner, mover, and leaver activities throughout these complex, fast-paced, and ever-changing lifecycles while maintaining granular control and visibility.

Higher education institutions face an array of challenges when it comes to securing access to their systems.

These include:

- Poor (or non-existent) visibility across a university's complex ecosystem of roles and identities for students, staff, and alumni.
- Disparate solutions for identity management, application access, and privileged access management (PAM) across both on-premises and cloud-based applications.
- A changing operating environment that includes third-party access by research and industry collaborators.

Emerging identity governance challenges require innovative approaches that are scalable and on-demand. Saviynt's cloud-based solution enables universities to manage their complex identity lifecycles in a secure and flexible way. Amid a changing business landscape, better identity management improves both today's and tomorrow's access challenges

The Challenging Identity Management Needs of Universities

During the past two years digital transformation and delivery programs, including access to remote learning, have been fast-tracked due to the pandemic. This rapid change resulted in a more complex operating environment for both enabling IAM for staff and students and also balancing the need for personal connection that comes with the traditional face-to-face experience.

The higher education sector has numerous specific requirements for identity and access governance in addition to those seen in a traditional enterprise.

As far back as 2015, higher education IT publication EDUCAUSE reported on the benefits of federated identity as an enabler for education[1] and, more recently, in February 2022 reported on the central role of IGA in a zero-trust architecture for cyber security[2]. According to that report, getting federated identity right is critical to maintaining the privacy of community participants and supporting their ability to create, educate, and collaborate.

"Threats could be anywhere and your intranet is likely no safer than the internet... but with modern technology that integrates and automates the environment, the environment is easier to manage and protect," according to the 2022 report.

Universities must manage access to corporate administration systems while providing a platform for a complex access network that includes students, staff, and industry collaborators.

[1] https://er.educause.edu/articles/2015/1/federated-identity-as-an-enabler-for-education
[2] https://er.educause.edu/articles/2022/2/zero-trust-architecture-rethinking-cybersecurity-for-changing-environments

The challenging identity management needs of universities include:

User experience: Today's sophisticated users expect a seamless onboarding experience. Problems or undue delays in accessing university systems can lead to a huge burden on the helpdesk and support staff. An inability to attach granular roles to a single identity can result in increased operating expenses and decreased productivity.

Multiple identity sources: Universities need to provide system and application access to staff, students, researchers, alumni, industry partners, third-party suppliers, and even volunteers. This level of diversity is well beyond what an average enterprise must deal with.

Rapid student access: Students need to be added and removed from online course material quickly and often for short periods of time. This calls for more automation and less manual intervention.

Changing roles: Students can teach and teachers can study. The role and needs of a person within a university's network can change quickly.

Data compliance: Universities still need to be compliant with the access and security of their data, particularly when it comes to attracting industry collaborators. Regulatory compliance such as FERPA, GDPR, PCI-DSS, ISO-27001, and SOX, can be achieved manually or with ready-to-go compliance controls and reporting frameworks such as the HECA Compliance Matrix.

Intellectual property: Universities have a comparatively high amount of research data and associated intellectual property. This requires access management across cloud and on-premises systems to be secured properly.

If universities are not able to manage their diverse identities coherently they risk losing opportunities to improve their internal operations. Additional risks include reduced quality of courses and research programs and non-compliance penalties.

From Code to Compliance: The Cost of Poor Identity Management

University leaders have a number of factors to consider when determining the real cost of disparate and ad-hoc identity management. They include manually performing identity and access governance responsibilities; using a combination of on-premises, homegrown tools that require internal coding; regular maintenance and upgrading; and significant management time if they were not cross-functional.

Furthermore, without unified identity management, universities are exposed to a high risk of security breaches and non-compliance postures, potentially resulting in audit fines and reputational damage.

In its 2020 report, The Total Economic Impact™ Of Saviynt Enterprise Identity Cloud, research firm Forrester found a typical enterprise (with less diversity than a university) experiences $34.5 million in time-cost over three years due to identity management inefficiencies and manual processes.

The cost analysis was performed across a number of key areas, including application access provisioning, segregation of duties management, improved access reviews, faster employee and contractor onboarding, and coding talent cost avoidance.

Failing to improve identity management will also increase risks as architectural landscapes become more complex.

A recent article by Gartner, IAM Leaders: Plan to Adopt These 6 Identity and Access Management Trends[3], highlighted the need to adopt six trends to improve identity management roadmaps and architecture in response to ongoing macroeconomic, organizational, and technology changes. These are:

- ✓ "Connect anywhere" computing will drive the need for smarter access control
- ✓ Improved user experience will be essential for secure digital business
- ✓ Keys, secrets, certificates, and machines will require more attention
- ✓ New applications and APIs will need to leverage the latest IAM development guidelines
- ✓ Hybrid cloud and multi-cloud will drive ongoing IAM architecture maintenance/evolution
- ✓ IGA functions will evolve to enable decentralized architecture

According to the report, "It is critical for security and risk management leaders to architect more flexible IAM infrastructure and for IAM teams to partner with other functions to meet changing organizational requirements."

It's clear that as digital transformation accelerates, security and identity are taking center stage as crucial components of an organization's business ecosystem. In one IDC report, Worldwide Identity and Access Management Market Shares, 2020: Continued Impact of COVID-19, 2020 was both a wake-up call and a mad scramble to do something significant to stop identity compromises, the top source of network attacks and data breaches.

[3] https://www.gartner.com/en/articles/iam-leaders-plan-to-adopt-these-6-identity-and-access-management-trends

How Universities Can Manage Complex Identity Lifecycles

Universities face increasing complexity managing their application delivery requirements and identity lifecycles. New approaches are needed to build long-term adaptability. IGA in a cloud and remote learning world calls for university IT and administration leaders to develop a broad strategy combining technology with organizational change.

Modern identity management and access control offer much more to the organization than an improved security posture. As you progress through your digital transformation journey, consider how an identity management platform can be a facilitator of change.

Review: Start with an assessment of how an identity management platform can improve security and user experience, which is important for a university's population.

Technology: Look to fit-for-purpose tooling that is designed to meet the complex identity needs of your university. The cost of not investing in the right technology can be much higher than the product itself or the risk of doing nothing.

Culture: Universities are part of a wide ecosystem and have many cloud and third-party access requirements. If the traditional approach was to manage IGA in-house, a cultural change might be needed to adopt a dedicated IGA solution. Adoption of cloud, remote learning, and industry collaboration in a structured way will be more sustainable than bespoke solutions.

Processes: Modern IGA offers more to a university than just access control. To get the most out of any solution, look for opportunities to automate manual processes and integrate new processes into your identity management needs.

Meeting the one identity for life goal will require you to think about how the university operates and what can be done differently.

How Technology Helps Deliver a Single Identity With Compliance

A cloud-native IGA platform offers a single, context-aware solution for your entire educational identity ecosystem. To help higher education institutions modernize identity governance, Saviynt IGA ensures users have seamless access to necessary resources on-premises, in the cloud, or in hybrid environments.

The platform increases organizational agility and operational effectiveness through automation and intuitive identity workflows. Powered by a comprehensive identity warehouse and an extensive controls library for risk-based, continuous compliance and security, Saviynt IGA is a core component to secure your move to cloud. Saviynt IGA also reduces the dependency on IT operations by empowering users and administrators with self-service features, providing a centralized control center to streamline administration, and reducing the digital fatigue of repetitive reviews.

Higher education institutions need to manage some of the most complex identity governance challenges. In this environment, not only is there a lot of coming and going, but people can also have multiple roles. A staff member could also be a student, for example. Things get even more complex because identities often originate from different systems. This illustrates why one identity for life is so important for universities.

To facilitate one identity for life, Saviynt IGA delivers granular visibility and is powered by a comprehensive identity warehouse and extensive controls, such as identity match and merge. With Saviynt, IT teams can contextually attach multiple personas and customized access permissions to a single identity that has complex scenarios.

In addition to identity management, university leaders must be able to demonstrate that effective security controls are in place and the institution is complying with privacy and data management regulations.

Identity isn't just creating and disabling an account. The modern focus is on having appropriate access at all times. Our built-in control center unifies identity administration by bringing together intelligence, reporting, and dashboarding to enable continuous compliance. After all, identity isn't just about creating and disabling an account. The modern focus is on having appropriate access at all times.

An always-ready compliance posture can also help attract government and private sector research grants. According to the Association of American Universities[4], funding decisions by federal agencies are based generally on a process of peer review, and compliance is monitored through a variety of audits conducted on a regular basis. Universities need to be ready to allow access to systems to stay in line with grant funding requirements.

Transform identity with a cohesive platform to manage your identity perimeter. Whether you need to enforce least privilege access, rein in third-party identity management, improve Separation of Duties (SoD) management or secure access to sensitive data, Saviynt can help you improve your university's security posture.

[4] https://files.eric.ed.gov/fulltext/ED517263.pdf

Forrester
The Total Economic Impact™ Of Saviynt Enterprise Identity Cloud
Cost Savings And Business Benefits Enabled By Enterprise Identity Cloud
DECEMBER 2020

Counting the savings and benefits enabled by Saviynt Enterprise Identity Cloud

With a combination of customer interviews and financial analysis, a 2020 Forrester Research study commissioned by Saviynt found that a large organization, such as a university, experiences benefits of $34.4 million over three years versus costs of $10.14 million with a cloud-based, digital identity and access governance platform. This adds up to a net present value (NPV) of $24.3 million and an ROI of 240%.

Saviynt in Action at The University of Canterbury

The University of Canterbury in New Zealand is an excellent example of how modern identity and access management meets the needs of a diverse community and improves business operations.

Saviynt helped the university build a centralized, streamlined IGA hub to facilitate automation, self-service account provisioning, and role-based access controls across an inherently complex higher education environment.

The University of Canterbury is New Zealand's second-oldest institution of higher learning and, like many others, the university provides IT resource access to a large and particularly dynamic user population.

Legacy Systems Held Back Transformation

Digital transformation, including the growth of online learning, degree programs, and massive open online courses (MOOCS), was the reality in higher education even before the onset of the COVID-19 pandemic. As a result, the university recruited a digital leadership team that crafted a new vision for digital transformation to enable the university to stay current with technological trends.

But the university's identity and security teams were impeded by a bespoke legacy IGA solution that also created visibility challenges. It required extensive coding and other manual steps before accounts could be provisioned and de-provisioned.

And one user can also have varied roles. It's not uncommon for students to also serve as research assistants or temporary staff, or for employees to enroll in courses. To support this diversity the university's teams must manage "joiner, mover, and leaver" identities throughout these ever-changing lifecycles, while ensuring that they can maintain granular control and visibility.

In today's increasingly cloud-centric and digital-first world, these time-consuming, labor-intensive processes were ineffective and burdensome.

A Single Identity For Life: Automation & Governance With Saviynt

With its operations held back by manual processes, the university turned to Saviynt IGA to automate access provisioning while centralizing identity information within a central repository. This repository serves as a single source of truth for the entirety of every user's identity journey, no matter how complex. According to Clive Keylar, IAM and Middleware Manager, The University Of Canterbury, in universities, the concept of one identity for life is fundamental.

"This is because a single person can have so many different roles and identities over the course of their relationship with the institution," he says. "They can be a student at the same time that they're a staff member, and then become an alumnus."

Saviynt’s cloud-native Identity Governance and Administration (IGA) solution has become the single source of truth for identity information across the University of Canterbury’s entire IT ecosystem. With this solution, the university has:

- **Faster onboarding:** New user onboarding and new account provisioning used to take hours and was typically done overnight. It can now be completed in 20 minutes.
- **Better visibility:** Saviynt IGA enabled enhanced visibility across all roles, identity types, and resources in the environment.
- **Application integration:** Saviynt seamlessly integrated cloud and on-premises resources, including the University’s Oracle PeopleSoft ERP implementation and a custom student management system (Jade).
- **Reduced administration:** The university saved time, streamlined processes, and reduced administrative overhead with Saviynt.
- **Access control platform:** The university can now implement role-based access controls, new workflow approval automation, and enterprise service management integrations.

With Saviynt’s IGA solution, the University of Canterbury has set a firm foundation for its digital future. The university now benefits from centralized identity governance to support future digital transformation, privilege management, and access control initiatives.

> **“Saviynt essentially makes it possible for us to assign people — with multiple, complex, changing personas — a single identity for life.”**
>
> - Clive Keylar, IAM and Middleware Manager, The University Of Canterbury

Saviynt IGA also boosted efficiency by automating processes, saving time, and reducing labor costs, so university staff, professors, students, IT, and business teams can focus on their primary goals: improving teaching and learning.

Conclusion

From digital transformation to pandemic countermeasures, the world's universities have been through unprecedented change during the past two years. To better manage this evolution, university leaders must meet their specific requirements for identity and access governance, from corporate systems to new ways to access digital services — including cloud-based remote learning and industry collaboration. To achieve one identity for life, higher education institutions need to be adaptable to complex identity governance challenges and identities which originate from aging disparate systems and new initiatives.

The world's leading analyst firms agree: The cost of improving IGA will be far less than the risk of continuing with a disparate approach — which is also less secure and difficult to manage in a changing digital landscape. IGA in a cloud and remote learning world calls for university IT and business leaders to develop a broad strategy that combines technology with cultural and process change. As the University of Canterbury has shown, operations do not need to be held back by manual processes.

Saviynt's IGA technology can automate access provisioning while centralizing identity information. Universities can create one repository that serves as a single source of truth for the entirety of every user's identity journey, no matter how complex. Everything from faster student onboarding to seamless application integration for corporate IT staff can be achieved with a modern, cloud-based IGA platform.

Now is the time to review the benefits identity management can bring to your university. Accelerate one identity for life adoption, protect student and faculty data, and simplify management to achieve an always-ready compliance posture with Saviynt.

Saviynt

Headquarters, 1301 E. El Segundo Bl, Suite D,
El Segundo, CA 90245, United States
310. 641. 1664 | info@saviynt.com
www.saviynt.com